

2/13/2006

In the Claims

Please cancel claims 1—82.

~~1~~ ~~83.~~ (New) A method, at least partially implemented by a computer, comprising:

building a data block comprising a first random value and a cryptographic hash of the first random value;

generating, on a second computing device, a signature by digitally signing a string containing a second random value; and

computing an encryption key, for encrypting the data block, by hashing a combination of the signature and a third random value.

~~2~~ ~~84.~~ (New) The method as recited in Claim ~~83~~, wherein the second computing device is a smart card.

~~3~~ ~~85.~~ (New) The method as recited in Claim ~~83~~, wherein the combination of the digitally signed string and the third random value comprises the digitally signed string concatenated to the third random value.

~~4~~ ~~86.~~ (New) The method as recited in Claim ~~83~~, wherein the combination of the digitally signed string and the third random value comprises the third random value concatenated to the digitally signed string.

1 ~~5~~ 87. (New) The method as recited in Claim ~~83~~<sup>1</sup>, further comprising:  
2 encrypting the data block using the encryption key; and  
3 storing the encrypted data block and the second and third random values.

4  
5 ~~6~~ 88. (New) The method as recited in Claim ~~87~~<sup>5</sup>, further comprising:  
6 accessing the stored encrypted data block and the second and third random  
7 values;  
8 providing a string containing the second random value to the second  
9 computing device; and  
10 generating, on the second computing device, a second signature by digitally  
11 signing the string containing the second random value.

12  
13 ~~7~~ 89. (New) The method as recited in Claim ~~88~~<sup>6</sup>, further comprising:  
14 computing a decryption key using the second signature and the third  
15 random value;  
16 decrypting the encrypted data block with the decryption key; and  
17 comparing the decryption of the encrypted data block to the data block.

18  
19 ~~8~~ 90. (New) The method as recited in Claim ~~89~~<sup>7</sup>, wherein computing the  
20 decryption key comprises:  
21 hashing the second signature concatenated to the third random value.  
22  
23  
24  
25

1 <sup>9</sup>~~91.~~ (New) The method as recited in Claim <sup>7</sup>~~89~~, further comprising:

2 hashing the first random value contained within the decryption of the  
3 encrypted data block; and

4 comparing the result of this hash with the hash of the first random value  
5 contained within the decryption of the encrypted data block.

6 <sup>10</sup>~~92.~~ (New) A method, at least partially implemented by a computer,  
7 comprising:  
8

9 accessing an encrypted data block, wherein the encrypted data block  
10 comprises an encryption of a combination of a first random value and a hash of the  
11 first random value;

12 accessing second and third random values;

13 providing a string containing the second random value to a second  
14 computing device;

15 generating, on the second computing device, a signature by digitally  
16 signing the string containing the second random value; and

17 computing a decryption key, configured to decrypt the encrypted data  
18 block, wherein computing the decryption key uses the signature generated on the  
19 second computing device and the third random value.

20 <sup>11</sup>~~93.~~ (New) The method as recited in Claim <sup>10</sup>~~92~~, wherein the second  
21 computing device is a smart card.  
22  
23  
24  
25

12  
94. (New) The method as recited in Claim 92, wherein computing the  
decryption key comprises:

hashing the signature concatenated to the third random value.

13  
95. (New) The method as recited in Claim 92, further comprising:  
decrypting the encrypted data block with the decryption key, wherein the  
first random value and the hash of the first random value are recovered by the  
decryption; and

comparing the first random value and the hash of the first random value  
recovered from the decryption to a data block from which the encrypted data block  
was generated.

14  
96. (New) The method as recited in Claim 95, further comprising:  
hashing the first random value recovered from the decryption of the  
encrypted data block; and

comparing the result of this hash with the hash of the first random value  
recovered from the decryption of the encrypted data block.

1 <sup>15</sup>  
2 ~~97.~~ (New) One or more computer-readable media comprising computer-  
3 executable instructions for encryption-based authentication, the computer-  
4 executable instructions comprising instructions for:

5 building a data block comprising a first random value and a cryptographic  
6 hash of the first random value;

7 generating, on a second computing device, a signature by digitally signing a  
8 string containing a second random value; and

9 computing an encryption key, for encrypting the data block, by hashing a  
10 combination of the signature and a third random value.

11 <sup>16</sup>  
12 ~~98.~~ (New) The one or more computer-readable media as recited in Claim  
13 ~~97~~, wherein the second computing device is a smart card.

14 <sup>17</sup>  
15 ~~99.~~ (New) The one or more computer-readable media as recited in Claim  
16 ~~97~~, wherein the combination of the digitally signed string and the third random  
17 value comprises the digitally signed string concatenated to the third random value.

18 <sup>18</sup>  
19 ~~100.~~ (New) The one or more computer-readable media as recited in Claim  
20 ~~97~~, wherein the combination of the digitally signed string and the third random  
21 value comprises the third random value concatenated to the digitally signed string.  
22  
23  
24  
25

19

~~101.~~ (New) The one or more computer-readable media as recited in Claim

97, further comprising instructions for:

encrypting the data block using the encryption key; and

storing the encrypted data block and the second and third random values.

20

~~102.~~ (New) The one or more computer-readable media as recited in Claim

~~101,~~ further comprising instructions for:

accessing the stored encrypted data block and the second and third random values;

providing a string containing the second random value to the second computing device; and

generating, on the second computing device, a second signature by digitally signing the string containing the second random value.

21

~~103.~~ (New) The one or more computer-readable media as recited in Claim

~~102,~~ further comprising instructions for:

computing a decryption key using the second signature and the third random value;

decrypting the encrypted data block with the decryption key; and

comparing the decryption of the encrypted data block to the data block.

1 <sup>22</sup>  
2 <sup>21</sup> ~~104~~. (New) The one or more computer-readable media as recited in Claim  
3 ~~103~~, wherein computing the decryption key comprises instructions for:  
4  
5 hashing the second signature concatenated to the third random value.

6 <sup>23</sup>  
7 <sup>21</sup> ~~105~~. (New) The one or more computer-readable media as recited in Claim  
8 ~~103~~, further comprising instructions for:  
9  
10 hashing the first random value contained within the decryption of the  
11 encrypted data block; and  
12  
13 comparing the result of this hash with the hash of the first random value  
14 contained within the decryption of the encrypted data block.  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

24  
106. (New) One or more computer-readable media comprising computer-executable instructions for encryption-based authentication, the computer-executable instructions comprising instructions for:

accessing an encrypted data block, wherein the encrypted data block comprises an encryption of a combination of a first random value and a hash of the first random value;

accessing second and third random values;

providing a string containing the second random value to a second computing device;

generating, on the second computing device, a signature by digitally signing the string containing the second random value; and

computing a decryption key, configured to decrypt the encrypted data block, wherein computing the decryption key uses the signature generated on the second computing device and the third random value.

25  
107. (New) The one or more computer-readable media as recited in Claim 106, wherein the second computing device is a smart card.

26  
108. (New) The one or more computer-readable media as recited in Claim 106, wherein computing the decryption key comprises instructions for:

hashing the signature concatenated to the third random value.



1 <sup>27</sup>  
2 ~~109~~ (New) The one or more computer-readable media as recited in Claim  
3 <sup>24</sup>  
4 ~~106~~, further comprising instructions for:

5 decrypting the encrypted data block with the decryption key, wherein the  
6 first random value and the hash of the first random value are recovered by the  
7 decryption; and

8 comparing the first random value and the hash of the first random value  
9 recovered from the decryption to a data block from which the encrypted data block  
10 was generated.

11 <sup>28</sup>  
12 ~~109~~ (New) The one or more computer-readable media as recited in Claim  
13 <sup>27</sup>  
14 ~~109~~, further comprising instructions for:

15 hashing the first random value recovered from the decryption of the  
16 encrypted data block; and

17 comparing the result of this hash with the hash of the first random value  
18 recovered from the decryption of the encrypted data block.

19 <sup>29</sup>  
20 ~~111~~ (New) A system configured for encryption-based authentication,  
21 comprising:

22 means for building a data block comprising a first random value and a  
23 cryptographic hash of the first random value;

24 means for generating, on a second computing device, a signature by  
25 digitally signing a string containing a second random value; and

means for computing an encryption key, for encrypting the data block, by  
hashing a combination of the signature and a third random value.

1 <sup>30</sup>  
2 ~~112~~ (New) The system as recited in Claim <sup>29</sup>~~111~~, wherein the second  
3 computing device is a smart card.

4 <sup>31</sup>  
5 ~~113~~ (New) The system as recited in Claim <sup>29</sup>~~111~~, wherein the combination  
6 of the digitally signed string and the third random value comprises the digitally  
7 signed string concatenated to the third random value.

8 <sup>32</sup>  
9 ~~114~~ (New) The system as recited in Claim <sup>29</sup>~~111~~, wherein the combination  
10 of the digitally signed string and the third random value comprises the third  
11 random value concatenated to the digitally signed string.

12 <sup>33</sup>  
13 ~~115~~ (New) The one or more computer-readable media as recited in Claim  
14 <sup>29</sup>~~111~~, further comprising:

15 means for encrypting the data block using the encryption key; and  
16 means for storing the encrypted data block and the second and third random  
17 values.

1 <sup>34</sup>  
2 ~~116.~~ (New) The system as recited in Claim ~~115~~<sup>33</sup>, further comprising:  
3 means for accessing the stored encrypted data block and the second and  
4 third random values;  
5 means for providing a string containing the second random value to the  
6 second computing device; and  
7 means for generating, on the second computing device, a second signature  
8 by digitally signing the string containing the second random value.

9 <sup>35</sup>  
10 ~~117.~~ (New) The system as recited in Claim ~~116~~<sup>34</sup>, further comprising:  
11 means for computing a decryption key using the second signature and the  
12 third random value;  
13 means for decrypting the encrypted data block with the decryption key; and  
14 means for comparing the decryption of the encrypted data block to the data  
15 block.

16 <sup>36</sup>  
17 ~~118.~~ (New) The system as recited in Claim ~~117~~<sup>35</sup>, wherein computing the  
18 decryption key comprises:  
19 means for hashing the second signature concatenated to the third random  
20 value.  
21  
22  
23  
24  
25

37  
119. (New) The system as recited in Claim 117, further comprising:  
means for hashing the first random value contained within the decryption of  
the encrypted data block; and  
means for comparing the result of this hash with the hash of the first  
random value contained within the decryption of the encrypted data block.

38  
120. (New) A system configured for encryption-based authentication,  
comprising:  
means for accessing an encrypted data block, wherein the encrypted data  
block comprises an encryption of a combination of a first random value and a hash  
of the first random value;  
means for accessing second and third random values;  
means for providing a string containing the second random value to a  
second computing device;  
means for generating, on the second computing device, a signature by  
digitally signing the string containing the second random value; and  
means for computing a decryption key, configured to decrypt the encrypted  
data block, wherein computing the decryption key uses the signature generated on  
the second computing device and the third random value.

39  
121. (New) The system media as recited in Claim 120, wherein the  
second computing device is a smart card.

38

40 38  
1 ~~122.~~ (New) The system as recited in Claim ~~120~~, wherein computing the  
2 decryption key comprises:

3 means for hashing the signature concatenated to the third random value.

41 38  
5 ~~123.~~ (New) The system as recited in Claim ~~120~~, further comprising:  
6 means for decrypting the encrypted data block with the decryption key,  
7 wherein the first random value and the hash of the first random value are  
8 recovered by the decryption; and

9 means for comparing the first random value and the hash of the first  
10 random value recovered from the decryption to a data block from which the  
11 encrypted data block was generated.

42 41  
13 ~~124.~~ (New) The system as recited in Claim ~~123~~, further comprising:  
14 means for hashing the first random value recovered from the decryption of  
15 the encrypted data block; and

16 means for comparing the result of this hash with the hash of the first  
17 random value recovered from the decryption of the encrypted data block.  
18  
19  
20  
21  
22  
23  
24  
25